STATE OF CALIFORNIA
OFFICE OF THE ADJUTANT GENERAL
P.O. Box 214405 - 2829 Watt Avenue
Sacramento, California 95821-0405

CAL ARNG Regulation
No. 18-1

1 September 1989

Army Automation
MICROCOMPUTER OPERATIONS POLICY

This regulation implements and supplements AR 380-380 and AR 25-1. Further supplementation to this regulation is prohibited without prior written approval from this headquarters.

		Paragraph	Page
CHAPTER 1	**General**		
	Overview Statement	1-1	1-1
	Purpose	1-2	1-1
	Objectives	1-3	1-1
	Responsibilities	1-4	1-1
CHAPTER 2	**Operational Policy**		
	General Policy	2-1	2-1
	Acquisition	2-2	2-2
	Standardization	2-3	2-3
	Training	2-4	2-3
	Documentation	2-5	2-3
	Equipment Installation	2-6	2-4
	Maintenance	2-7	2-5
	Operational Consideration	2-8	2-5
CHAPTER 3	**Security & Accreditation Policy**		
	Accountability	3-1	3-1
	Security Consideration	3-2	3-1
	Accreditation Process	3-3	3-1
	Computer Contaminates	3-4	3-2
APPENDIX A	**Facility Security Profile**		A-1
APPENDIX B	**Short Form Risk Assessment**		B-1
APPENDIX C	**Sensitivity Designation**		C-1
APPENDIX D	**Password Receipt**		D-1
APPENDIX E	**Abbreviated Mission Element Needs Statement**		E-1
APPENDIX F	**Facility Security Profile / Annex**		F-1

CAL ARNGR 18-1
C-1

STATE OF CALIFORNIA
OFFICE OF THE ADJUTANT GENERAL
2829 Watt Avenue
P.O. Box 214405
Sacramento, California 95821-0405

Change
No. 1

22 September 1989

Army Automation
MICROCOMPUTER OPERATIONS POLICY

1. CAL ARNGR 18-1, 1 September 1989, is changed as follows:

   Remove first and last pages and insert new first and last pages, attached.

2. File this change in front of the publication for reference purposes.

(CAIM)

BY ORDER OF THE GOVERNOR:

ROBERT C. THRASHER
Major General
The Adjutant General

OFFICIAL:

CURWOOD F. REYNOLDS
COL, INF, CAL ARNG
Administrative Officer

OF CALIFORNIA
OFFICIAL COPY

DISTRIBUTION:
A
M
NGB-IMA - 5
6th Army DOIM - 5

CHAPTER 1
General

1-1. GENERAL. Microcomputer technology has brought Automated Data Processing (ADP) capabilities via small computers into the functional user's office area, significantly enhancing human productivity. Microcomputers are defined as a laptop, portable, personal [desktop] computer and the super-micro computer [eg. INTEL 310/320]. These systems are defined as electronic data processing devices using one or more microprocessors and selected peripherals for input, storage, manipulation and output of information. Battlefield automated systems fall under this regulation for security only. Maintenance and training are outside the scope of this regulation.

1-2. PURPOSE. This policy provides guidance for managing, acquiring, accrediting, operating and securing microcomputer assets within the California Army National Guard (CA ARNG).

1-3. OBJECTIVES. The objective of this policy is to provide uniform procedures to:

a. Accommodate an orderly application of the CA ARNG microcomputer program.

b. Promote the use of command standard hardware.

c. Promote the use of off-the-shelf command standard software.

d. Ensure the required ADP support, training, and equipment are given to the functional users.

e. Ensure CA ARNG compliance with current NGB, Army, DOD and State Administrative Manaual information management policies and directives.

f. Provide guidance for these additional duty assignments: Information Management Officer [IMO], ADP System Security Officer [ADPSSO], ADP Point of Contact [ADPPOC], and the Terminal Area Security Officer [TASO].

1-4. RESPONSIBILITIES. To provide the most efficient application of the CA ARNG microcomputer program, the following responsibilities are assigned:

a. Director of Information Management (DOIM):

(1) Provides approval of staff/unit microcomputer requirements in accordance with AR 18-1, AR 25-1, AR 380-380, and CA ARNG Information Management Plan (IMP).

(2) Provides training and assistance in procuring and using off-the-shelf hardware and software.

(3) Assists functional personnel in formulating applications on the microcomputers and solving technical problems.

(4) Serves as the Adjutant General's technical advisor for computer activities.

(5) Researches and develops computer standards to ensure compatibility.

(6) Coordinates the development of long range computer related budget requirements.

(7) Assists the staff/unit in developing computer related requirements.

(8) Approves communication software packages.

(9) Advises and assists functional users in regard to security and accreditation requirements of AR 380-380.

b. The Information Management Officer (IMO) is appointed to:

(1) represent the information requirements of each of the Directorate Staff, Senior Commands, and the Brigade level commands of the 40th INF DIV (M). The IMO may hold any rank in the organization.

(2) understands the Information Mission Area (IMA) function within the organization.

(3) responsible for Information Management planning, identification of requirements and coordination of these requirements within his/her organization.

(4) submit requirements through the DOIM for consolidation of State IMA needs.

(5) if appointed, act as member of the Information Management Advisory Council (IMAC). As such, will be able to review and arbitrate on local technical issues, and represent his/her organizational requirements.

c. Every activity/unit having: Terminals, Microcomputer or, Minicomputers will designate an individual who will act as ADP Point of Contact (ADPPOC) for ADP related activity.

(1) The ADPPOC will ostensibly be an individual who is computer literate or who is expected to be the designated computer literate person.

(2) The ADPPOC should be familiar with all references within this document.

(3) The ADPPOC may hold any rank in the organization, however, the POC will recognize and be guided by the organization IMO, ADPSSO and TASO.

(4) Serve as the interface between the functional user and the IMO for all microcomputer activities.

(5) Notify the respective IMO immediately of any problems encountered with the microcomputer (e.g., hardware, software, communications, etc.). After notifying the SRCOM or Directorate IMO, notify the DOIM.

(6) Be responsible for obtaining accessory equipment within their scope of responsibility (e.g., furniture, dust covers, signs, etc.). All software and/or hardware requests must be sent to the DOIM through the SRCOM IMO. This request must outline the product(s) desired, a justification for each item, and a POC [if other than the ADPPOC].

(7) Ensure site preparation actions have been initiated prior to or in conjunction with Automated Data Processing Equipment (ADPE) delivery.

(8) Request additional hardware/software in accordance with procedures identified in paragraph 6.

(9) Provide the DOIM, through the command's IMO, copies of new or updated software applications for the CA ARNG application directory.

~~(10) Coordinate and manage functional area software.~~

(11) Coordinates with the SRCOM's IMO & ADPSSO in all matters pertaining to the preparation and submission of accreditation documentation.

d. Senior Commands and BDE level commands of the 40th ID (M) will appoint Automated Data Processing Systems Security Officers (ADPSSO's). The ADPSSO will:

(1) Function on behalf of the commander as the point of contact for all aspects of automation security. This position is an additional duty.

(2) Cause operations to be partially or completely suspended upon detection of any action which may affect the security of the operations. This suspension will remain in effect until removed by the commander. The ADPSSO must be given written authorization by the appointing authority to suspend access to any system subscriber.

(3) Ensure implementation of automation security regulations by:

(a) Preparing, distributing, and maintaining plans, instruction, and guidance, and/or standard operating procedures (SOPs) concerning the security of automated operations.

(b) Conducting periodic surveys or reviews to determine compliance with such regulations.

(c) Conducting reviews of threats and vulnerability so as to enable the SRCOM commander to properly assess risks, and determine effective measures to minimize such risks.

(d) Coordinating any changes in the security environment with the State System Security Manager.

(4) Report immediately to the facility manager and State System Security Manager any attempt to gain unauthorized access to sensitive defense information or any system failure or suspected defect which could lead to unauthorized disclosure.

(5) Take measures to protect the physical facility.

(6) Review and evaluate the security impact of system changes, including interfaces with other automated systems.

(7) Insure that a TASO is properly appointed in writing for each terminal or group of contiguous terminals. (Applies only to multi-user microcomputers, and minicomputers.)

(8) Coordinate and monitor periodic security indoctrination and training sessions for assigned personnel.

(9) Have the capability to audit or review every file within the system without obtaining prior permission from the file owner within a multi-user computer environment.

(10) Compile accreditation documentation to accompany the commander's request for accreditation from the appropriate accreditation authority.

(11) Advise the DOIM / DPI Chief of available INSCOM automation security services. The ADPSSO will request such support in the event of serious system security deficiencies of hazards, or discovery of a security incident or violation.

(12) Conduct, from a security viewpoint, a daily review of audit trail and other system management or user access reports.

(13) Issue and control physical access authorization of personnel with a demonstrated requirement to enter the activity or site (including users, contractors, and maintenance personnel). The ADPSSO will also maintain records of validated access authorizations within a multi-user computer environment.

(14) Compile and maintain the Facility Security Profile (FSP) described in Appendix F.

(15) Control and manage the generation and issuance of system passwords.

(16) Review annually the requirements for each Limited Access Authorization (LAA).

(17) Review quarterly the physical inventory of magnetic media in accordance with AR 18-7.

e. The ADPSSO of multi-user computers will appoint a Terminal Area Security Officer (TASO). The TASO who is appointed for the remote terminals and interface device(s) connected with a host computer. He/she will:

(1) Ensure that written instructions are issued specifying security requirements and operating procedures for each terminal area.

(2) Ensure that each terminal user's identity, need-to-know, level of security clearance, and access authorization is established commensurate with the data available for that terminal.

(3) Manage the control and dissemination of user or file identification and passwords.

(4) Implement controls to prevent entry of unauthorized transactions or data (such as, classified data over unsecured data transmission lines) through the remote terminal.

(5) Ensure local compliance with automations security procedures.

(6) Assist the host system ADPSSO in providing system security.

(7) As soon as possible, report to the host system ADPSSO all practices dangerous to system security, and all security violations.

CHAPTER 2
OPERATIONAL POLICY

2-1. GENERAL POLICY. a. The acquisition, management and use of computers is subject to existing Federal Acquisition Regulation (FAR), DA Automation Regulations, the Army Microcomputer Buy, and supplemental policy contained herein. The CA ARNG microcomputer policy is based on centralized review of all acquisitions, and decentralized management and use.

b. The DOIM has the authority to approve microcomputer resource acquisitions only if authorized by a TDA. Software acquired in support of the microcomputers will not duplicate present or planned Army Standards Systems or existing CA ARNG automated systems. Additionally, newly acquired microcomputer hardware will be compatible with currently installed microcomputer systems.

c. Implementation of off-the-shelf software is the responsibility of functional users (end-users). Custom designed programs will, as a general rule, be developed by end-user programmers with assistance from the DOIM Information Center. The DOIM will provide maintenance support for functional user developed programs, provided proper documentation is supplied in accordance with paragraph 2-7.

d. Access to other CA ARNG systems data.

(1) A microcomputer with dial-up communications capabilities functions as a computer terminal when accessing another computer system. The telecommunications service manager on the DOIM staff will set up, manage and monitor all telecommunication (TC) operations for remote users. The ADPSSO/TASO at the off-site site has similar "networking" responsibilities.

(2) System access shall be restricted to terminal emulation as described above. Only approved communications software packages shall be used to accomplish this function.

e. Classified or Privacy Act Information.

(1) Classified Information. Classified information is not authorized for processing on the microcomputer without prior approval of the State System Security Manager [CA ARNG]. The accreditation document will include classified processing considerations. Classified information will be processed in approved facilities only. If Tempest equipment is determined to be necessary, submit an acquisition request in accordance with the Abbreviated Mission Element Needs Statement (AMENS) Appendix E to this regulation.

(2) Personnel Data. All users must safeguard systems with personnel data according to the Privacy Act of 1984, Public Law 93-597, Title 5 USC. The ADPSSO or TASO will provide guidance to develop and implement Privacy Act operating instructions in accordance with AR 340-21.

f. Software Piracy.

(1) Laws. Users will read and comply with the software license agreements. This includes prohibitions against copying materials (disk and manuals) legally protected by copyrights and using software on more than one PC. If multiple copies are needed ***they must be purchased.*** It is unlawful to copy / reproduce

copyrighted computer programs without proper authority. Limitations and restrictions are imposed by the copyright license agreement of each program. This prohibition includes not only copying for personal use but also copying for use in legitimate applications. All software loaded on the hard disk must have its particular manual(s) co-located with the personal computer. Manuals not co-located with the system potentially indicates that the system has illegally copied software resident on that system. Lost manuals should be reported to the IMO for replacement.

(2) Copying. Some licenses allow a user a backup or archival copy to have on hand in case the program disk is damaged. Making copies to share with other computer users, or copying a program at work to use at home, is forbidden.

g. Privately Owned Computers. ***The use of privately owned microcomputers is highly discouraged.***

h. Personal Use of Government Owned Computers. The government provides computer resources for the accomplishment of official duties. The use of government owned computers in support of private/personal programs/endeavors is expressly forbidden. Such programs/endeavors are defined to include personal use, by clubs or other organizations, companies, games, or any other activity which does not specifically support the conduct of business for the California Army National Guard. Violation will be reported to the State ADP System Security Officer.

2-2. ACQUISITION. a. When a requirement has been identified by the functional user that lends itself to microcomputer processing, the functional user will forward a request (through channels) in accordance with the Abbreviated Mission Element Needs Statement (AMENS) Appendix E, for microcomputer hardware and/or software to the DOIM. The request must state the intended use, justification for the requirement and a brief benefit and/or cost analysis. The DOIM will review to insure the request complies with the CA ARNG Information Management Plan (IMP) and that the equipment will meet the user needs and minimum standards.

b. After reviewing, the DOIM will forward the Abbreviated Mission Element Needs Statement (AMENS) to NGB-IMA for approval and addition of the equipment to the STARC TDA. An information copy will be sent to the USPFO [ATTN: CAUS-SC-MI].

c. CA ARNG will follow the current guidelines for procurement of PC's and will meet the minimum standards established by NGB.

d. Directorates or Senior Commands (SRCOMs) with funding available for transfer should initiate the requests indicated in paragraph 2-2a. above and contact the DOIM. This will expedite the acquisition of your microcomputer assets. If a QRIP proposal is used to fund an acquisition, one should first contact the DOIM for assistance/guidance. The DOIM's approval is also required for all QRIP proposals for administrative equipment.

e. Procurement procedures are as follows:

(1) SRCOMS / Directorate submits request and justification to the DOIM.

(2) DOIM approves and obtains approved AMENS from NGB-IMA.

(3) SRCOMS / Directorate submits DD Form 1348-6 and approved AMENS to USPFO [CAUS-SU] for procurement action. If funds transfer is required, it must be accomplished prior to this step. If QRIP is used to fund, QRIP must be approved by the DOIM-CA and funds received from DA prior to this step.

(4) Upon receipt of the equipment, the DOIM, or his designated representative (reference paragraph 4b), will unpack and install the equipment. No other individual will unpack or attempt installation of the equipment, as CA ARNG risks invalidating equipment warranty if specific instructions are not followed. The DOIM has these instructions and has been thoroughly briefed in the initial installation. While the DOIM is installing the equipment, the receiver will sign and forward the appropriate documents to USPFO for action.

2-3. STANDARDIZATION. It is important that the microcomputer technology acquired within National Guard enhances the ability of decision makers to share and exchange information. Achievement of this objective will be possible only by adherence to the following principles of standardization.

a. Software Applications. Software applications will not duplicate present or planned National Guard standard applications. DOIM maintains a list of software applications. That list should be reviewed before initiating any new development.

b. Hardware/Software. Efforts must be made to ensure computer hardware/software is standardized and compatible throughout the command. The DOIM is responsible for the identification of microcomputer resources (hardware and software) which will be compatible with existing CA ARNG computer equipment.

c. Naming Conventions. Care must be exercised when writing programs to use standard names and formats for data fields. The AR 18-12 series and functional guidance (ARs, ADSMs, etc.) should be consulted. Proposals for standard data elements should be submitted through functional channels.

d. Library. Reference library, (e.g., User's Guide, System Reference Manual's, FM's, Computer Books/Manuals) can be obtained through the DOIM Training Center.

2-4. TRAINING. a. Users will be provided with vendor documentation for necessary hardware and software operation (e.g., User's Guide, System Reference Manual, and Owner Manual). It is the responsibility of the user to read and understand the necessary manuals prior to using the microcomputer system. Users are also responsible for maintaining and safeguarding the manuals. Manuals will be located near the personal computer they came with. Lost or damaged manuals will be handled IAW AR 735-5.

b. The DOIM will schedule formal software training on a periodic basis. ADPPOCs will coordinate with their respective SRCOM IMO for training allocations and availability. Units will follow command channels to request support.

2-5. DOCUMENTATION. a. Microcomputer applications developed by the functional users will be documented. This user documentation will provide the potential user of the application with necessary information to understand and efficiently use the application. User documentation is an important tool for personnel training, it also facilitates software sharing, maintenance and validation. Properly documented applications can help in alleviating the impact of personnel turnover training.

b. Documentation will be prepared as applications are developed. The documentation will include, as a minimum, the following items:

(1) Application's Function. An Application Description [AD] must be completed and maintained in the functional area and a copy provided to the DOIM.

(2) System Operation. A user's guide will be prepared for each application program. The user's guide will:

(a) Supply information on how to load, set up, and run the program.

(b) Include an explanation of valid responses, available options and their output, input data required for processing, and interface with other programs.

(c) Identify any constraints in the capability or use of the program.

(d) Include a description of any data files used, data file layout, and data elements with definition.

(e) Describe error messages and required corrective measures.

2-6. EQUIPMENT INSTALLATION. a. Location of the Microcomputer. Microcomputers will run in any comfortable environment. An acceptable environment must be determined by referencing the manufacturer's warranty requirements and following these general guidelines:

(1) It is the unit ADPPOC's responsibility to coordinate with the DOIM for the installation of newly acquired equipment. The DOIM will provide technical assistance for all installations where required.

(2) It is the directorate/unit responsibility to ensure that the equipment is physically secure.

(3) Microcomputers can be operated on an office table or desk. Special purpose furniture to provide additional physical security or mobility is available through local procurement channels.

(4) The area in which the microcomputer is located will be as dust free as possible.

(5) Static electricity can destroy internal components and render the microcomputer useless. Static electricity is major concern in dry locations and carpeted rooms. Antistatic mats should be acquired.

(6) Locating the PC by windows should be avoided because of their vulnerability to forced entry, observation, solar heating problems and water leaks.

(7) The location of the equipment in the center of the work area is highly desirable so that the maximum protection provided by the building can be obtained. The environment above, below, and adjacent to the area should be also considered.

b. Installation Briefing. The DOIM staff and/or the IMO will brief the user on the use of the new equipment/software being installed. While this briefing will not provide all the training the user will need, it should serve as a basis to allow initial utilization of the equipment without damage.

c. Electrical System. While plans do not currently call for extensive rewiring of facilities for the purpose of PC installation, every effort should be made to obtain clean power with minimal electrical interruption from outside sources (eg. coffee pots, etc.). In locations where this becomes impossible, the unit will request assistance through Facilities Branch. Only the surge protectors and printer may be plugged directly into the wall circuit. All other devices (microcomputer, modem, buffers, etc.) will be plugged into the surge protector. This is to protect the equipment in the event of a power surge or power outage.

2-7. MAINTENANCE. a. The DOIM will insure that proper maintenance support, including preventative maintenance, is budgeted.

b. The SRCOM IMO will be contacted immediately if there are any problems with hardware or software not designated for use in a tactical environment. Maintenance shall only be authorized by the DOIM. The SRCOM or Directorate IMO will contact the DOIM with any problems.

c. Microcomputers will not be used in a "tactical field" environment due to the risk of possible abuse which may void the maintenance agreement and could make the hand-receipt holder responsible for the cost of repairs. Such damage to microcomputers would also cause costly down-time for users, and loss of data.

d. If microcomputers need to be moved from home station to a training site during periods of AT or IDT, they will only be used in appropriate buildings in a "garrison" environment and extreme care must be taken in transportation of them to and from training sites. Improper use, care, or transportation of these microcomputers during such periods may void the maintenance agreement and could make the hand-receipt holder responsible for the cost of repairs. Any such move must first be approved by the SRCOM IMO with an information copy furnished to the DOIM [CAIM-M].

e. Original equipment packing cartons and material shall be kept and used for transportation of ADPE to and from home station.

2-8. OPERATIONAL CONSIDERATION. a. Powering Up/Down. Specific instructions involving the steps to be followed during the power up/down sequence of a microcomputer are contained in the operations manuals. Adherence to these procedures is ***MANDATORY***. Failure to comply with those procedures could result in damage to the computer, its peripherals, and software. Additionally, resulting in a loss of data.

b. Diskettes. Diskettes are precision recording media and can be easily damaged. The following procedures on the care and maintenance of diskettes must be followed.

(1) Keep the diskette in its storage envelope or holder when not in use.

(2) Keep diskettes away from any magnetic fields, as strong magnetic fields will erase data stored on a diskette.

(3) Do not touch the exposed area of diskette or try to wipe or clean them. Diskettes scratch easily.

(4) Diskettes must be kept out of the sun and away from extreme heat and cold.

(5) Do not write on the diskette jacket with a ball point pen, lead pencil, or other hard point devices; ***ONLY A FELT TIP PEN WILL BE USED.***

(6) Diskettes should be stored vertically in a file folder to avoid pressure to their sides.

(7) Diskettes will be protected from theft by securing them in a locked area when left unattended.

c. Backup Diskettes. Each unit is required to maintain at least one [1] backup of the entire hard disk. This mandatory complete backup will be no older than 30 days. Each unit is also required to maintain a complete backup of all diskettes used to store data/documents, etc. This mandatory complete backup of disks will be no older than 30 days. These complete backups should be stored in an alternate site from where the PC(s) are located. Backup copies of data should be made more frequently and consistently because a power failure or spilled cup of coffee could destroy months worth of data instantly. Backing up data after each use and deleting files from the hard disk will allow many users access to the PC. Several large applications will quickly fill available space on the hard disk. Original copies of applications and backup diskettes should be kept in a DOIM approved safe area.

d. Miscellaneous Information. Dust can damage computers. Dust covers or a sheet of plastic will help alleviate this problem. Any substance that could damage microcomputers must be kept clear of it at all times. Users will not eat, drink, or smoke in the vicinity of the equipment. Appropriate signs to this effect should be posted in the area of the computer.

CHAPTER 3
SECURITY AND ACCREDITATION POLICY

3-1. ACCOUNTABILITY. A microcomputer is governed by applicable NGB and Army regulations dealing with property accountability of ADP equipment. Requirements for obtaining approval/authorization, purchase, and property book accountability will be in accordance with AR 710-2, DA Pam 710-27, AR 310-34 and AR 310-49. Sixth US Army is required by the Headquarters, Department of the Army (HQDA) to maintain for information and analysis purposes Automated Data Processing Equipment (ADPE) inventories. ADPE must be accounted for and entered into the ADPE inventory system as required. The DOIM will be responsible for ensuring that all ADPE is properly entered into the inventory system. The unit Property Book Officer is accountable for assigned ADP equipment.

3-2. SECURITY CONSIDERATIONS. a. General. All computer areas will be secured upon the completion of the duty day or at any time the facility is unoccupied, such as during a fire drill, bomb threat, etc. Only authorized users are allowed to use hardware in conjunction with his/her duties. Computer systems will be secured in a facility which takes at least two locked doors, etc. to gain access to the PC.

b. Security of CPU, Printer and Keyboard. The System, at minimum, will be secured by LOCKED doors at the end of the duty day. Approved items such as "Anchor Pads" provide additional security.

c. Floppy Disk. Floppy disks will be secured in a locked cabinet or desk drawer. Software must be kept under close and continuous control to insure that unauthorized changes are not made.

d. Classified Information Disk. Classified information will only be processed on computers in accordance with AR 380-380 and AR 530-4. Master copies of application software used to process classified information or other data and documentation supporting that software will be secured and/or otherwise protected as prescribed by AR 380-5. Master floppy diskettes should be locked in a DOIM approved safe area during non-duty hours. Classified data will not be stored on any hard disk at any hour. A sign-out log sheet will include name, grade, organizations, security clearance, program name, time in, access system and time out.

3-3. ACCREDITATION PROCESS. a. Accreditation is the critical review of a designated automated system prior to operation. It will provide the accreditation authority (DOIM-CA) information to determine that sensitive information can be processed within the bounds of acceptable risk. The accreditation document will be forwarded to the DOIM for determination of sensitivity level of operation and accreditation approval. All computer systems within the CA ARNG will be accredited.

b. The accreditation process requires, as a minimum, investigation, information gathering, and formal review by management at both the operating and accrediting levels.

c. Accreditation should evolve from the following actions as fully outlined in AR 380-380, and in accordance with Appendix A through C of this regulation.

(1) Statement of accreditation goals and objectives, to include, a validation of the need for the operations requiring this accreditation.

(2) Detailed risk management review to identify risks and alternatives available to counter risks.

(3) Detailed description of proposed operations, to include key security features forming the basis of accreditation.

(4) Plan for implementation and review of additional security features.

(5) Plan for systems security test and evaluation.

(6) Statement of continuing problem areas, resource requirements and impacts, and milestone schedule, if appropriate. Since the documentation associated with the formal accreditation describes in detail the vulnerability, risks, system design and physical layout of the system, consideration should be given to classifying such documentation at a level commensurate with the classification of information in the system. As a minimum, the documentation will be considered "FOR OFFICIAL USE ONLY" [FOUO]. Access to accreditations will be on a "need-to-know" basis and will be maintained by the DOIM-CA.

3-4. COMPUTER CONTAMINATES. a. Compute contaminates are defined as any program or series of instructions which alter the structure of the system, destroy data or programs or generally deny access to the system for any period of time [eg. viruses, worms, logic bombs, etc.].

b. Any system operator/user who discovers a potential contaminate affecting the system [eg. lost data, extremly sluggish performance, or messages which randomly pop up on the screen, etc.] will report this situation to his/her respective ADPSSO.

c. The ADPSSO will in turn contact the State System Security Manager and report the following information:

(1) Computer model number and serial number of each piece of equipment connected to the suspected system.

(2) The reporting user, his/her phone number and the unit's ADPPOC and phone number.

(3) Description of the problem.

d. Under no circumstance will the user of the suspected system use that system after the incident is reported. If the system is infected with a contaminate, any additional use where trading data disks between systems takes place, may contaminate those other systems.

e. The system, upon remote evaluation by the State System Security Manager, may have to be shipped to the DOIM for further inspection. Specific instructions will be issued on a case-by-case basis by the SSSM.

APPENDIX A
FACILITY SECURITY PROFILE (FSP)
(Appendix D, AR 380-380)

A-1. FACILITY IDENTIFICATION AND LOCATION:

a. Organization/Activity/Unit: ______________________________

b. Building Number/Floor/Room(s) ______________________________

A-2. DIAGRAM OF SYSTEM LAYOUT: See paragraph A-9

A-3. ADPE DESCRIPTION:

a. System Name: ______________________________

b. Manufacturer: ______________________________

c. Model: ______________________________

d. Series: ______________________________

A-4. INVENTORY OF SYSTEM HARDWARE: See Page A-4

A-5. SYSTEM TELECOMMUNICATIONS CAPABILITIES (Actual or Proposed):

a. Does this system utilize a modem? ______________________________

b. Make/Model of modem utilized: ______________________________

c. Is this telecommunications system connected via:

Dial-up telephone: ______________________________

Auto-dial modem: ______________________________

Direct-wired: ______________________________

d. This system utilizes: (Answer "yes" or "no" for each)

DES encryption device(s)	yes / no
KG-type encryption device(s)	yes / no
Other form of encryption device(s)	yes / no

e. Does this system process "record telecommunications" (para 1-9, AR 530-2)? yes / no If "yes", and no encryption devices are utilized, does this system operate under an AR 350-2 waiver? yes / no Attach a copy of operating waiver or statement that no waiver exists.

f. If this system is part of a network (on or off-post), provide a diagram of the network to include remote terminal configuration to include:

APPENDIX A (continued)

(1) Unit/activity operating the network.

(2) Location of all terminals operated by activity/organization.

A-6. CATEGORIES OF INFORMATION/DATA PROCESSED BY THIS SYSTEM:

Use AR 380-5 definitions only. Express each category as a percentage with the sum of all categories equal to 100 percent.

a. TOP SECRET (TS) para 1-501, AR 380-5 ______________%

b. SECRET (S) para 1-502, AR 380-5 ______________%

c. CONFIDENTIAL (C) para 1-503, AR 380-5 ______________%

d. UNCLASSIFIED (U) ______________%

TOTAL: 100 percent

Categories of unclassified information/data processed by this system: (Answer "yes" or "no" for e through k below)

e. Large dollar volume assets/resource accounting authorization data of an amount of at least $25 million per annum (para 1-8a, A 380-380. yes / no

f. Large dollar volume assets/resource accounting, authorization data of an amount less than $25 million but greater than $1 million per annum (para 1-8b(3), AR 380-380. yes / no

g. FOR OFFICIAL USE ONLY (FOUO AR 340-17) yes / no

h. Privacy Act of 1975. yes / no

i. Contract Management. yes / no

j. Proprietary. yes / no

k. FOR TRAINING USE ONLY (FTUO) yes / no

A-7. INVENTORY OF SYSTEM'S SOFTWARE: See Page A-7

A-8. PERSONNEL SECURITY AND SURETY PROGRAM (PSSP).

a. Number of personnel authorized to operate this system:________

b. Number of security clearance (by type) of authorized system users:

(1) TOP SECRET (TS):________________

(2) SECRET (S):____________________

(3) CONFIDENTIAL (C):______________

(4) NO CLEARANCE:_________________

APPENDIX A (continued)

c. Status of personnel without valid security clearance:

(1) Number of personnel with completed NAC, ENTNAC, or NACI investigation but no clearance issued. ____________________

(2) Number of personnel with pending NAC, ENTNAC, or NACI investigation. ____________________

(3) Number of personnel without NAC, ENTNAC, or NACI initiated/pending. ____________________

d. Organization/Unit/Activity Security Manager [ADPSSO, TASO, etc.]:

(1) Name:____

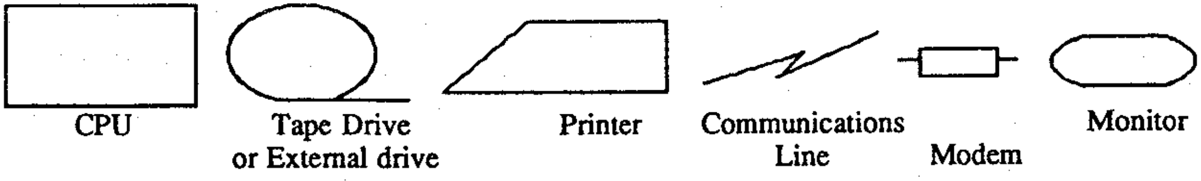
(2) Telephone Number: (   ) ____-__________ [AV] ____-__________

(3) Office Symbol: ______________

A-9. PHYSICAL SECURITY PROGRAM: Complete Appendix H, Automation Security Checklist, AR 380-380 and include it in your accreditation package.

INSTRUCTION - DIAGRAM OF SYSTEM LAYOUT

1. Use a separate sheet of paper for your diagram of your ADPE system.
2. Use dotted lines to show boundaries of rooms/buildings.
3. Do *not* show electric power wiring.
4. Use the following symbols for your diagram:



5. Identify all symbols with a model/series identifier.
6. Identify fully, any symbols not identified in #4, above.
7. Diagram does *not* need to be to scale.
8. Equipment identified on diagram should be consistent with the FSP.

APPENDIX A (continued)
INVENTORY OF SYSTEM HARDWARE

	Manufacturer	Model/Series	Serial Number	Location/Room(Bldg)	Remarks
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					

APPENDIX A (continued)
INVENTORY OF SYSTEM SOFTWARE (Commercial)

	Name	Manufacturer	Quantity	Remarks
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				

APPENDIX B
SHORT FORM RISK ASSESSMENT

DATE:____________________

1. ACTIVITY/LOCATION: ____

2. CONTACT/NAME: ____

3. PHONE NO:(   ) ______-________ [AV] ______-____________

4. EQUIPMENT LOCATION: ____

5. SYSTEM IDENTIFICATION: ____

6. SYSTEM DESCRIPTION (SYSTEM COMPONENTS): Reference Page A-1 thru A-2 paragraphs A-3, A-5, A-6, A-8 of this regulation.

7. APPLICATION, CLASSIFICATION, AND PERCENTAGE OF PROCESSING TIME:
(Utilization) 5 days - 8 hrs to 7 days - 24 hrs

MODE: (Check one) (   ) SYSTEM HIGH (   ) DEDICATED

CLASSIFICATION* (PERCENT)

TYPE	TS	SE	CO	SB	PA	FOUO	UN
A. Engineering							
B. Personnel							
C. Inventory Control, Inventory							
D. Maintenance, PPC							
E. Financial/Budget							
F. Administrative							
G. Contractual							
H. Management Information							
I. Other: R & D (Application-Programs)							

*TS = Top Secret; SE = Secret; CO = Confidential; SB = Sensitive Business; PA = Privacy Act; FOUO = For Official Use Only; UN = Unclassified

APPENDIX B (continued)

8. INFORMATION STORED (In the computer or on magnetic storage media; tapes, disk, diskettes). Percentage of all storage available.

CLASSIFICATION* (PERCENT)

TYPE TS SE CO SB PA FOUO UN

A. Personnel ________________________

B. Inventory ________________________

C. Financial/Budget ________________________

D. Contractual ________________________

E. Management Information ________________________

F. Engineering ________________________

G. Maintenance, PPC ________________________

H. Administrative ________________________

I. Other (Programs, Operating System) ________________________

J. Extra for Growth ________________________

9. Data Value. This section will be completed by the Accreditation Manager, DOIM-CA.

(1) TOTAL ACCESSION COSTS FOR DATA $ ________________________
(Data Value)

(2) REPLACEMENT OF LOST DATA (easy, difficult, impossible):________________

(3) IF INVENTORY OR FINANCIAL/BUDGET PROCESSING OR FILES ARE USED, GIVE TOTAL DOLLAR VALUE INVOLVED $ ____________________

10. TOTAL VALUE OF SYSTEM (i.e., acquisition cost of all hardware and software. This section will be completed by the Accreditation Manager, DOIM-CA.)

A. GOVERNMENT-OWNED; PURCHASE PRICE $____________________

B. LEASED, LEASE COST $ ______________ Month:____________ Year:______

11. TEMPEST TEST

A. HAS BEEN REQUESTED (DATE REQUESTED?) ____________________

B. HAS BEEN PERFORMED (DATE AND RESULTS?) __________________

APPENDIX B (continued)

12. SCOPE OF SYSTEM:

A. STAND ALONE: ( ) REMOTE CAPABILITY EXISTS, BUT NOT CURRENTLY IN USE.

B. TIED TO REMOTE COMPUTER (IDENTIFY SYSTEM/SHOW PERCENTAGE OF TIME).

13. PERSON WITH SECURITY COGNIZANCE OVER SYSTEM AND DATA:

A. NAME: ____

B. PHONE: (___) ____-__________ [AV] ____-__________

C. TITLE: ____

14. SYSTEM USERS (NAME): ____________________________________

15. THREATS/COUNTERMEASURES; FOR EACH THREAT, INDICATE ALL COUNTERMEASURES THAT APPLY:

a. Threat: FIRE

1. Sprinklers Installed	( ) Building	( ) Immediate Area
2. Halon installed	( ) Building	( ) Immediate Area
3. Fire extinguishers	( ) Building	( ) Immediate Area
4. Fire bell available	( ) Building	( ) Immediate Area
5. Smoke detectors installed	( ) Building	( ) Immediate Area
6. Fire alarm	( ) Building	( ) Immediate Area
7. Other	( ) Building	( ) Immediate Area

b. Threat: POWER LOSS

1. Back-up power available
2. Non-volatile memory
3. Auto-restart
4. Auto logging (audit)
5. Not significant (Can only check if auto-restart and auto-logging is also indicated).
6. Other

c. Threat: WATER DAMAGE

1. Computer location
2. Raised floor
3. Humidity indicator(s)
4. Dry pipe sprinkler
5. Water damage highly unlikely

d. Threat: LOSS OF DATA INTEGRITY

1. Security procedures
2. Operating procedures (proper data entry)
3. Air conditioning
4. Anti-static measures (use of spray chemicals, humidifiers etc.)

APPENDIX B (continued)

e. Threat: UNAUTHORIZED USE

1. Passwords (machine generated)
2. O.S. Security incorporated
3. Administrative
4. Physical isolation/protection

f. Threat: PHYSICAL PENETRATION

1. Cipher locks
2. Recognition
3. Parameter fence
4. Security guards
5. CCTVs
6. Security awareness (indoctrination)
7. Key locks
8. Combination locks
9. Area alarms
10. Other

g. Threat: DISGRUNTLED EMPLOYEE

1. High morale
2. Good attitude
3. Growth potential
4. Close supervision
5. Training

12. Contingency Planning (mission criticality)

a. Not required as loss of processing capability for a reasonable period of time would not adversely affect mission.

b. Required since loss of processing capability for even a short period of time would adversely affect mission.

1. Plan is in existence.
2. Plan is being developed
3. To date no action has been taken to develop a plan.

13. Comments (site-unique security related matters not covered above):
(COOP) Continuity of Operations Considerations.

14. PREPARED BY:________________________ DATE:________________

Signature: _____________________________

APPENDIX C
SENSITIVITY DESIGNATION

C-1. FACILITY/SYSTEM:

a. Unit/Office: ____________________

b. Location (building and room number): ____________________

c. ADPSSO, TASO, or ADPPOC: ____________________

C-2. MISSION: (Provide a brief description of the system mission, include a list of programs)

C-3. EQUIPMENT INVENTORY: (List ADP equipment, e.g., CPU, keyboard, CRT, tape drive, disk drive, including all terminals and locations connected to the system, Indicate the make and model number of each item of equipment.)

C-4. VALUE OF SYSTEM: (Indicate approximate dollar value of all system components, including commercial software packages. This section will be completed by the Accreditation Manager, DOIM-CA)

C-5. STORAGE MEDIA: (List types of storage media and number by category)

	DISK	TAPES
Secret		
Confidential		
Asset/Resource		
Privacy Act		
FOUO		
Other		
TOTAL		

C-6. ESTIMATED VALUE OF ASSET/RESOURCE ACCOUNTING DATA PROCESSED: (Indicate approximate dollar value of asset/resource accounting or authorization data processed by the system at any one time. Indicate a minimum and maximum range expected at any one time during the year.)

C-7. AMOUNT/TYPE OF SENSITIVE PROCESSING: (Approximate number of hours processed in each category per week or month)

Secret
Confidential
Privacy Act
Asset/Resource
Other

____

TOTAL PROCESSING (week or month)

C-8. MISSION ESSENTIAL: (Is the system mission essential? Are adequate backup systems, manual or automated, in place to continue operations in the event of primary system failure?)

APPENDIX C (continued)

C-9. CURRENT SECURITY PROCEDURES IN EFFECT: Describe security procedures and controls in following areas, as applicable.

a. Physical Security

b. Personnel Security

c. Communications Security

d. Emanations Security

e. Hardware Security

f. Software Security

g. Procedural Security

C-10. RECOMMENDED SENSITIVITY DESIGNATION: ____________________

____

C-11. REMARKS: (Any additional information that should be considered in the determination of the sensitivity level of this equipment.)

APPENDIX D
PASSWORD RECEIPT

I hereby acknowledge personal receipt of the system password(s) associated with the USER-IDs listed below. I understand that I am responsible for the password(s) protection, will comply with the instructions provided me, and will not divulge them to any unauthorized person. I further understand that I should report to an appropriate security officer (TASO or ADPSSO) any problem I may encounter in the use of the password(s) or any misuse of password(s) by other persons.

SYSTEM USER-ID

____________________ ____________________

____________________ ____________________

____________________ ____________________

____________________ ____________________

____________________ ____________________

____________________ ____________________

Signature: ____________________ Date: __________

____

(First name, Middle initial, Last name, Grade/Rank)

Organization: ____________________ Duty phone: ( ) _____-__________

[AV] _____-__________

APPENDIX E
ABBREVIATED MISSION ELEMENT NEEDS STATEMENT (AMENS)

DATE:______________________
Activity:____
Address:____
____

Point of Contact:________________ [Comm] ___-___-______ [AV] ___-_______

1. Need. (Outline the need for microcomputer automation as related to specific elements of the activity's mission. Briefly summarize the functional requirement and the information dependent tasks that a microcomputer would process. Describe the current method and evaluate the impact on operations of maintaining the status quo capability)

2. Proposed Solution. (Summarize the selected configuration from the standard Army contract, including software, intended to satisfy the information processing need and identify various assumptions and constraints, if any, considered in the selection. Indicate milestone schedule of planned events, e.g., target dates for acquiring equipment and implementing various applications.)

3. Other Alternatives Considered. (Summarize other alternative configurations considered and explain why each was not selected as a proposed system.)

4. Cost and Benefits. (Summarize the cost of the proposed system and identify the expected benefits, i.e., improvements to functional support and cost savings.)

5. Interface Considerations. (Describe planned and potential interface and communication requirements both external and internal to the organization.)

6. Funding. (Identify the source and type of funding available for the proposed system.)

7. Acquisition Strategy. (The ISSAA Contract DAHC 26-85-D-0005 will be cited for the Intel 310 Contract with SMS or the ISSAA Contract DAHC 26-85-D-0006 for the Wang PC Contract with Automated Data Management (ADM). Other contract numbers will be provided when (and if) additional standard contracts are awarded.)

8. Other Comments. (Including any additional information that will facilitate understanding and evaluating this AMENS. Training, security/privacy, maintenance, and site preparation requirements should be addressed in this section.)

9. **Joint Signature.**

Functional Requirement Validated by:____________________________ date:__________

Deployment / Acquisition of System Approved: ________________________________

Approving Authority:______________________ date:_________

APPENDIX F
FACILITY SECURITY PROFILE ANNEX [FSP-A]

F-1. The purpose of the FSP is to describe and document the physical facility, equipment components, their locations and relationships, general operating information, and other characteristics relevant to the security of the facility and its operations.

F-2. The FSP will be used by the ADPSSO and other security personnel as the basis for estimating security needs, performing security assessments, identifying possible vulnerability, and facilitating risk management or accreditation efforts.

F-3. No changes may be made to facilities and configurations as documented in the FSP without coordination with the ADPSSO. The FSP should be of sufficient detail as to enable detection of changes which would affect the overall security of the facility or the basis of original accreditation.

F-4. The FSP, because of the comprehensiveness of system and facility documentation contained therein, should be protected by a security classification, if appropriate. At a minimum, the FSP will be handled as FOR OFFICIAL USE ONLY information (exemption categories 2 and 5, AR 340-17, para 3-200 apply), kept under positive control, and accessed only on the basis of strict need-to-know.

F-5. The following outline should be used as a guide in compiling FSP information. As a general rule, the more sensitive the DPA or ATS, the more extensive the documentation should be.

a. Facility identification and location.

b. Architectural drawings or building plans. Plans of the building housing the facility should show the locations of exits, guard posts, fire alarms and hoses, master utility panels, and facilities adjacent to, above, and below the DPA or ATS.

c. Facility floor plan. The floor plan will show placement of all equipment, desks, cabinets, tables, fire extinguishers and sprinklers, smoke and motion detection devices, emergency lighting, and so forth.

d. System logical interface diagrams. The diagram will show all major equipment (processing units, terminals, peripherals, communications modems, controllers, or concentrators, transmission lines, line filters, encryption devices, and so forth), and their interfaces.

e. Other diagrams. If applicable, diagrams will show specialized displays of communications, electrical wiring, special communications switching, or patching panels.

f. Equipment inventories. All ADP/ATS and related equipment will be inventoried by manufacturer type and model number. Specialized support equipment such as degaussers and tape and disk cleaners will be included.

g. Storage media. Types (magnetic tapes, disk packs) and approximate numbers will be shown by sensitivity category (for example, magnetic tapes-total 1,000; 25 SECRET, 50 CONFIDENTIAL, 25 Privacy information, 100 asset/resource information, 800 other.)

APPENDIX F (continued)

h. Amounts and types of sensitive processing. Wall clock time will be used to estimate processing time for each classification and restrictive category of information.

i. Executive software.

(1) Operating system. List the release or level number and date first put into operation on the system.

(2) Operating system type. Describe if standard off-the-shelf or the nature of any local modifications.

(3) Other major executive software. For example, list supervisors, non-hardware input/output controllers, query language processors, teleprocessing packages, and output spooling routines.

j. Utility software.

(1) Data management systems or data base management systems. Identify vendor, system name, release number, and date made operational.

(2) Other major utility software. List general software which supports both executive and applications software (such as, sort/merge routines, interpreters, compilers, converters, and report or report program generators).

k. Applications software. List the major applications programs or systems, indicating average processing time, security level, and/or restrictive category (such as, privacy information, asset, or resource information).

(CAIM)

BY ORDER OF THE GOVERNOR:

ROBERT C. THRASHER
Major General
The Adjutant General

OFFICIAL:

JOHN D. TYRRELL
LTC (CA), FA, CAL ARNG
Chief, Office of Administration

DISTRIBUTION:
A
M
NGB-IMA - 5
6th ARMY DOIM - 5